A.D

R E P U B L I Q U E F R A N Ç A I S E

PCT/FR 99 / 0 1 8 2 6

09/744652

4 FR99/1826

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

REC'D 20 SEP 1999
WIPO PCT

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 31 AOUT 1999

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA REGLE 17.1.a) OU b)

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

DB 267/250298
ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

THIS PAGE BLANK (USPTO)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITE

cerfa N° 55 -1328

Code de la propriété intellectuelle-Livre VI

REQUÊTE EN DÉLIVRANCE

28 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 27. JUIL 1998

N° D'ENREGISTREMENT NATIONAL 98 09575

DÉPARTEMENT DE DÉPÔT

DATE DE DÉPÔT 27 JUIL. 1998

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Cabinet BALLOT-SCHMIT
16, Avenue du Pont Royal
F-94230 CACHAN
FRANCE

LB/pl

n°du pouvoir permanent — références du correspondant 014134/FR — téléphone 01 49 69 91 91

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale: ☒ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☒ différé ☐ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

Procédé de contrôle de l'exécution d'une demande d'actions transmise par un serveur vers une carte à puce via un terminal.

3 DEMANDEUR (S) n° SIREN — code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

GEMPLUS

Forme juridique

S.C.A.
(Société en Commandite par Actions)

Nationalité (s) Française

Adresse (s) complète (s)

Avenue du Pic de Bertagne
Parc d'activités de la Plaine de Jouques
13420 GEMENOS

Pays

FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

BORIN Lydie
Mandataire N° 94-0506
Cabinet BALLOT-SCHMIT

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DIVISION ADMINISTRATIVE DES BREVETS
26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

N° D'ENREGISTREMENT NATIONAL
9809575

014134 LB/pl

TITRE DE L'INVENTION :

Procédé de contrôle de l'exécution d'une demande d'actions transmise par un serveur vers une carte à puce via un terminal.

LE(S) SOUSSIGNÉ(S)

Lydie BORIN

Cabinet BALLOT-SCHMIT
16, Avenue du Pont Royal
F-94230 CACHAN
FRANCE

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

DREHER Dominique
IMBERT Patrick

Domiciliés au : Cabinet BALLOT-SCHMIT
16, Avenue du Pont Royal
F-94230 CACHAN
FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Fait à CACHAN, le 27 Juillet 1998

L. Borin

BORIN Lydie
Mandataire N° 94-0506
Cabinet BALLOT-SCHMIT

BA 113/271196

PROCÉDÉ DE CONTROLE DE L'EXÉCUTION D'UNE DEMANDE D'ACTIONS TRANSMISE PAR UN SERVEUR VERS UNE CARTE A PUCE VIA UN TERMINAL

La présente invention concerne les systèmes d'échanges de messages entre serveur d'application et cartes à puce empruntant un réseau de communication. Elle s'applique aux échanges s'effectuant à travers les réseaux de télécommunication, réseau téléphonique commuté, réseau cellulaire ou réseau Internet. .

Généralement, les messages échangés entre un serveur d'application et l'application correspondante dans une carte à puce transitent par un équipement intermédiaire que l'on désignera par terminal dans la suite. La carte à puce d'un utilisateur coopère avec le terminal pour permettre les échanges.

Dans le cas où le réseau emprunté est un réseau de téléphonie, le terminal est un terminal de télécommunication. Dans le cas où le réseau emprunté est un réseau informatique, le terminal est un équipement informatique de type ordinateur équipé d'une interface de lecture/écriture de cartes à puce.

Un serveur sous contrôle d'un organisme émetteur de carte, désirant effectuer une action sécurisée dans une carte à puce (ou dans une application de ladite carte) via un réseau téléphonique, utilise des certificats cryptographique permettant d'assurer la sécurité des échanges.

Cependant, en cas de perte d'un message durant la transmission ou l'exécution ou en cas de tentative de fraude, la re-synchronisation des messages serveur-cartes peut poser des problèmes sécuritaires.

Dans le cas où le terminal est un terminal dédié et sécurisé sous contrôle de l'organisme émetteur (par

exemple un distributeur automatique de billets DAB sous contrôle d'une banque), la perte d'un message est compensée par des mécanismes de synchronisation mettant en jeu à la fois le logiciel du serveur et le logiciel du terminal dédié. Le terminal dédié est sécurisé soit physiquement (DAB) soit contient à l'intérieur un module SAM (Secure Authentication Module), et dans tous les cas est contrôlé étroitement par l'organisme émetteur.

Si le terminal utilisé n'est pas un terminal dédié et sécurisé (par exemple téléphone GSM, PC sous Internet,...), les mécanismes de synchronisation ne peuvent pas être basés sur la sécurité du terminal, du fait que celui-ci n'est pas contrôlable par l'émetteur.

En effet, il est important de pouvoir re-synchroniser la source des messages et la carte à puce en cas de problème de transmission sur le réseau. Ce problème a été posé en terme de sécurité vis-à-vis des opérateurs et des fournisseurs de service.

Il n'existe pas à ce jour de système prévu pour assurer une synchronisation entre la carte et le serveur, dans les cas où pendant une transaction en cours, acceptée par conséquent par la carte, le serveur profite de la connexion pour envoyer un message comportant une ou plusieurs actions à mettre en oeuvre par la carte, ces actions pouvant être par exemple un rechargement d'unités de valeur ou de paramètres (monétaires ou autre) ou un chargement d'une nouvelle application.

En effet, il est prévu dans le cadre plus général des cartes multi-applicatives, que des message soient envoyés alors que l'utilisateur a fait une demande de transaction afin d'envoyer des commandes pour des

actions à entreprendre pendant le déroulement de l'application pour la transaction en cours.

De tels messages permettront par exemple de commander un rechargement de porte-monnaie électronique dans le cas d'une application porte-monnaie électronique, ou de modifier des paramètres bancaires de l'application bancaire, ou le chargement d'une nouvelle application dans la carte.

Il est clair que dans cette situation, le serveur ne sera pas informé dans le cas où ledit message est perdu.

En d'autres termes, effectuer des actions sécurisées sur un terminal non dédié est faisable aujourd'hui mais impose, soit des contraintes utilisateur fortes (cartes ou applications bloquées si l'action sécuritaire n'est pas parvenue à terme), soit des risques de perte d'informations (par exemple perte d'une transaction de rechargement d'un porte-monnaie électronique).

Le but de l'invention est que le serveur puisse détecter les défauts d'exécution d'une ou plusieurs actions ou commandes, liés à une perte de messages entre le serveur et la carte à puce ou à des défauts d'exécution d'actions dans la carte, lesdits messages ayant été transmis à la carte éventuellement pendant une transaction en cours, ceci afin d'en informer le serveur pour que ce dernier détermine quelles sont les dernières actions ou commandes non exécutées par la carte.

Selon une procédure pré-établie en fonction de la ou des actions non mises en oeuvre, le serveur pourra par exemple renvoyer le message contenant la dite ou les dites actions et permettre leur exécution.

A cette fin, l'invention a particulièrement pour objet un procédé de contrôle de l'exécution d'une demande d'actions transmise par un serveur vers une carte via un terminal, ladite carte comportant un compteur d'actions, caractérisé en ce qu'il comporte les étapes suivantes :

a) à l'émission par le serveur d'un message comportant une demande comprenant une ou plusieurs actions à mettre en oeuvre par la carte, le serveur stocke le nombre n d'action de la demande;

b) à la réception du message, la carte exécute successivement la ou les actions de la demande en incrémentant son compteur d'actions entre chaque actions si l'action s'est bien exécutée et en refusant cette action et les actions successives si l'action ne s'est pas bien exécutée sans incrémenter son compteur.

c) on compare la variation entre la valeur dans la carte et celle stockée dans le serveur et on détermine que les x dernières actions (commandes) ne sont pas exécutées si le résultat de la comparaison présente un écart de x.

L'incrémentation du compteur d'action correspond au nombre d'actions correctement exécutées.

Le nombre x est égal à 0 si toutes les actions sont correctement éxécutées, ce nombre x peut donc varier de 1 à n si la dernière ou toutes les actions ont échoué.

Pour comparer la variation entre la valeur dans la carte et celle stockée dans le serveur, la carte transmet au serveur la valeur courante de son compteur avant et après exécution de la commande d'actions.

Pour comparer la variation entre la valeur dans la carte et celle stockée dans le serveur, la carte calcule la valeur de la variation de son compteur suite

à l'exécution de la commande d'actions et la transmet au serveur.

Selon une autre caractéristique, tout échange de la valeur du compteur d'actions de la carte est effectué systématiquement de manière sécurisé.

A cette fin, la dernière valeur du compteur d'actions de la carte est transmise avec un cryptogramme dont le calcul implique la dite dernière valeur.

Selon une autre caractéristique la dernière valeur courante du compteur d'actions de la carte est transmise au serveur en temps réel, c'est-à-dire pendant la transaction en cours.

Selon un exemple la valeur pourra être transmise au moyen du message d'acquittement de la transaction en cours dans la carte.

Selon une autre caractéristique la valeur du compteur d'actions de la carte est transmise au serveur en temps différé.

Selon un exemple la valeur du compteur d'actions pourra être transmise au moyen d'un message d'une nouvelle demande de transaction par la carte par le serveur.

Selon un autre exemple la valeur du compteur d'actions de la carte est transmise au moyen d'un message d'information émis pour la carte au serveur.

L'invention a également pour objet une carte pour mettre en oeuvre le procédé précité comportant un compteur et des moyens de gestion de ce compteur, caractérisée en ce que lesdits moyens de gestion sont aptes à incrémenter ledit compteur d'actions entre chaque action si l'action s'est bien exécutées et à ne pas l'incrémenter pour cette action ni pour les actions suivantes si cette action n'a pas été exécutée.

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description ci-après donnée à titre d'exemple non limitatif et en regard des dessins sur lesquels :

- la figure 1, illustre des échanges de messages entre serveur et carte à puce selon l'invention,
- la figure 2, illustre de manière détaillée des échanges de messages entre serveur et carte à puce dans le cas d'une perte de message,
- la figure 3, illustre un autre cas de perte de message.

On entend par demande d'actions, un message comportant un jeu de n commandes, n pouvant bien entendu être égal à 1.

On pourra se reporter pour mieux comprendre la suite au schéma de la figure 1.

Dans toute la suite, on a pris comme exemple le cas où le serveur 2 profite d'une transaction en cours dans une carte 1 pour lui envoyer une demande comportant une ou plusieurs actions que la carte devra exécuter.

Bien entendu dans ce cas une demande d'action sera émise avec la réponse à la transaction en cours si ladite transaction nécessite une réponse. Si ce n'est pas le cas, crée une réponse contenant uniquement la demande d'actions. Le terminal qui est en communication avec le serveur reçoit le message correspondant à cette réponse, épure ce message de son enveloppe pour transmettre les actions à la carte.

Une demande d'actions peut comporter plusieurs actions à entreprendre par la carte, c'est-à-dire comme précisé au début de la description, un jeu de n commandes.

A titre d'exemple une demande d'actions pourra être une demande de changement d'un ou plusieurs paramètres dans un programme d'application ou, le chargement d'une nouvelle application ou, le chargement d'unités de valeur.

Le changement d'un paramètre correspond à une action pour la carte qui est une opération d'effacement et écriture à une adresse prédéterminée.

Le changement de plusieurs paramètres correspond à autant d'opérations d'effacement et écriture à des adresse distinctes que de paramètres et par conséquent à autant d'actions à entreprendre qu'il y a de paramètres à changer.

On va maintenant détailler ce qui se passe côté carte et côté serveur.

Côté carte :

La carte 1 incrémente après chaque action correctement effectuée, le compteur d'actions CA dès qu'elle reçoit du serveur une ou plusieurs actions à entreprendre et qu'elle a pu mener à bien l'exécution de chacune de ces actions.

La valeur du compteur est remontée vers le serveur par exemple chaque fois que la carte envoie un message au serveur (message 3 ou message 4 sur la figure 1).

La valeur du compteur peut être remontée vers le serveur 2 essentiellement lors des actions suivantes :

- lorsqu'il y a un acquittement de transaction (si durant une transaction un message d'acquittement est remonté au serveur on peut mettre dans cet acquittement la valeur du compteur d'actions), (exemple : message 3),
- lorsqu'il y a une demande de transaction ou d'authentification de la carte vers le serveur, (exemple : message 4),

- dans le cas de cartes bancaires ou de porte-monnaie électronique :

- on stocke dans chaque terminal 3 toute transaction passée,

- la transaction stockée est remontée au serveur pour que le serveur puisse enclencher le processus de paiement du marchand auprès duquel a eu lieu la transaction, le compteur d'actions CA peut être remonté avec cette transaction.

Ainsi, la valeur du contenu du compteur d'actions est toujours remontée au serveur soit en temps réel lorsque cela est fait lors d'un acquittement ou en temps différé lors d'une nouvelle demande de transaction ou lors d'une remontée d'un stockage de transactions.

Côté serveur :

Pour chaque carte contenant une application qui lui est dédiée ayant une demande d'actions en cours, le serveur doit stocker :

- le numéro d'identification de l'application,
- la valeur courante du compteur d'actions,
- la liste des actions en cours pour cette carte.

Ainsi, le serveur auquel appartient une application placée dans une carte à puce multi-applicative, peut lors de n'importe quelle transaction demandée par la carte, commander une action telle qu'un rechargement d'unités, ou qu'un chargement d'un programme ou qu'un chargement de nouveaux paramètres pour un programme résidant dans la carte.

Le serveur peut ainsi envoyer des actions à la carte par un mécanisme de script non interprétable par le terminal 3, qui se trouve entre le serveur et la carte pour assurer la communication. Le terminal 3

transmet le ou les messages reçus dans le script à la carte de manière transparente.

On va maintenant détailler l'ensemble des traitements dans le cas où la remontée du contenu du compteur d'actions se fait en temps réel et dans le cas où tout se passe bien, c'est-à-dire dans le cas où il n'y a pas de perte de message et où l'exécution par la carte s'est bien déroulée.

On pourra se reporter au mode de réalisation particulier illustré par le schéma de la figure 1 pour mieux comprendre.

- A l'instant dti le porteur demande via son terminal 3 une transaction (un paiement ou une autre transaction): message 1.

- La carte prépare la transaction et un cryptogramme, c'est-à-dire les données d'authentification, désignées par la suite par MAC et transmet au terminal.

Associé à cette transaction, l'application bancaire joint la valeur actuelle CA de son compteur d'actions sécurisé par le cryptogramme.

- Le terminal remonte la transaction au serveur bancaire.

De façon pratique, la carte envoie un message de demande de transaction contenant les données MAC1 ainsi que la valeur du compteur d'action CA, et l'identification de la transaction demandée.

- Le serveur vérifie les données d'authentification de la carte MAC1 et traite la transaction. Le serveur peut à ce moment effectuer une action dans l'application de la carte.

Selon un exemple particulier, il peut s'agir d'un chargement de paramètre monétaire dans la carte, mais

comme cela a été dit, d'autres actions du type rechargement d'un porte-monnaie électronique sont également possibles.

- Pour cela, le serveur va préparer une ou plusieurs commandes de chargement de paramètres contenues dans un champ d'information dénommé ci-après script 1, et les données d'authentification sécuritaire MAC2.

- La demande d'action est envoyée par un message 2 qui peut contenir la réponse à la transaction en cours si une telle réponse est prévue pour l'application concernée.

Au moment de l'envoi du script 1 à la carte, le serveur stocke dans une base de donnée ce script 1, en y associant les données relatives à la carte, ainsi que la valeur courante CA du compteur d'actions de la carte (remontée de la carte vers le serveur durant la demande de transaction). Ces informations vont permettre d'effectuer la synchronisation serveur-carte.

- La carte qui reçoit les commandes une à une du script 1, vérifie le cryptogramme MAC2, et effectue de manière atomique (c'est-à-dire en une fois et de manière indivisible) action par action de la liste du script 1 et incrémente le contenu CA du compteur après chaque action si celle-ci s'est bien déroulée. Lorsqu'une action s'est mal déroulée, le compteur d'action n'est pas incrémenté et les autres actions ne sont pas acceptées.

- Afin de remonter au serveur la nouvelle valeur CA' du compteur d'actions CA de la carte, plusieurs schémas sont possibles :

- remontée lors d'un message d'acquittement de la transaction en cours c'est-à-dire en temps réel, (correspond au message 3 de la transaction en cours);

- remontée de la valeur du CA' durant la prochaine transaction, (correspond au message 4 se produisant à l'instant dtj);

- à n'importe quel moment c'est à dire lorsque la carte envoie des informations au serveur.

- Dans le cas de l'exemple décrit, la carte renvoie un acquittement sécurisé au serveur incluant le contenu CA' en temps réel. Celui-ci peut alors comparer la valeur retournée par l'acquittement avec la valeur stockée dans sa base.

Si la valeur CA' = CA+n, n étant le nombres d'actions du script 1, ceci prouve que le script 1 s'est déroulé correctement dans la carte. Le serveur peut alors effacer ce script dans la base de données.

On va maintenant décrire en relation avec la figure 2, en reprenant le même exemple, ce qui se passe lorsque se produit une coupure ou une perte du message de demande d'actions (message 2).

Dans ce cas de figure, la commande script 1 n'est pas arrivée dans la carte. Le serveur va devoir se resynchroniser. Le serveur est informé de cette situation car selon cet exemple il n'a pas reçu d'acquittement.

Dans les cas où le serveur n'attend pas d'acquittement, il est informé lorsqu'il reçoit la dernière valeur du compteur d'action de la carte c'est à dire par exemple lors de la prochaine transaction.

En effet, durant l'authentification de la carte par le serveur (vérification MAC1), le serveur identifie que cette carte n'a pas reçu le script 1 (ou que le script 1 n'a pas été effectué correctement dans la carte) grâce à la valeur CA' du compteur d'actions qui

est remontée au serveur et comparée à la valeur CA stockée dans le serveur.

Si CA' est inférieur à CA et non égal, cela veut dire que la dernière ou les dernières actions n'ont pas été effectuées correctement.

Dans ce cas le serveur remet à jour sa base de données DB, en effaçant la valeur CA pour mettre la valeur CA'. Le serveur est à nouveau synchronisé et peut relancer la ou les dernières actions non exécutées par la carte.

On va maintenant décrire en relation avec la figure 3, en reprenant toujours le même exemple, ce qui se passe lorsque se produit une coupure lors du message d'acquittement.

Ce cas ne peut être envisagé que dans le cas où un message d'acquittement est prévu par l'application. Mais le même problème peut se produire lorsque la remontée du compteur d'actions est effectuée au moment d'une demande d'une nouvelle transaction, ou de l'envoi d'un message d'information.

Dans ce cas de figure, lors de la nouvelle demande de transaction, la valeur courante du compteur d'actions de la carte CA' = CA+n est remontée.

Le serveur compare cette valeur CA' à sa dernière valeur stockée, c'est-à-dire CA. Comme CA' = CA+n, le serveur sait que les n dernières actions ont bien été menées, il stocke la nouvelle valeur du compteur d'actions, c'est-à-dire CA+n pour être synchronisé avec la carte.

REVENDICATIONS

1. Procédé de contrôle de l'exécution d'une demande d'actions transmise par un serveur vers une carte via un terminal, ladite carte comportant un compteur d'actions, caractérisé en ce qu'il comporte les étapes suivantes :

a) à l'émission par le serveur d'un message comportant une demande comprenant une ou plusieurs actions à mettre en oeuvre par la carte, le serveur stocke le nombre n d'action de la demande;

b) à la réception du message, la carte exécute successivement la ou les actions de la demande en incrémentant son compteur d'actions entre chaque actions si l'action s'est bien exécutée et en refusant cette action et les actions successives si l'action ne s'est pas bien exécutée sans incrémenter son compteur.

c) on compare la variation entre la valeur dans la carte et celle stockée dans le serveur et on détermine que les x dernières actions (commandes) ne sont pas exécutées si le résultat de la comparaison présente un écart de x.

2. Procédé selon la revendication 1, caractérisé en ce que pour comparer la variation entre la valeur dans la carte et celle stockée dans le serveur, la carte transmet au serveur la valeur courante de son compteur avant et après exécution de la commande d'actions.

3. Procédé selon la revendication 1, caractérisée en ce que pour comparer la variation entre la valeur dans la carte et celle stockée dans le serveur, la carte calcule la valeur de la variation de son compteur

suite à l'exécution de la commande d'actions et la transmet au serveur.

4. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que la carte transmet ledites valeurs sous forme sécurisée.

5. Procédé d'échange de messages selon la revendication 1, caractérisé en ce que la valeur du compteur d'actions de la carte est transmise en temps réel, c'est-à-dire pendant la transaction en cours.

6. Procédé d'échange de messages selon la revendication 5, caractérisé en ce que la valeur du compteur d'actions de la carte est transmise au serveur au moyen du message d'acquittement de la transaction en cours dans la carte.

7. Procédé d'échange de messages selon la revendication 1, caractérisé en ce que la valeur du compteur d'actions de la carte est transmise en temps différé.

8. Procédé d'échange de messages selon la revendication 7, caractérisé en ce que la valeur du compteur d'actions de la carte est transmise au serveur au moyen d'un message d'une nouvelle demande de transaction par la carte pour le serveur.

9. Procédé d'échange de messages selon la revendication 7, caractérisé en ce que la valeur du compteur d'actions de la carte est transmise au moyen d'un message d'information émis par la carte au serveur.

10. Carte pour mettre en oeuvre le procédé selon l'une des revendications précédentes comportant un compteur et des moyens de gestion de ce compteur, caractérisée en ce que lesdits moyens de gestion sont aptes à incrémenter ledit compteur d'actions entre chaque action si l'action s'est bien exécutées et à ne pas l'incrémenter pour cette action ni pour les actions suivantes si cette action n'a pas été exécutée.

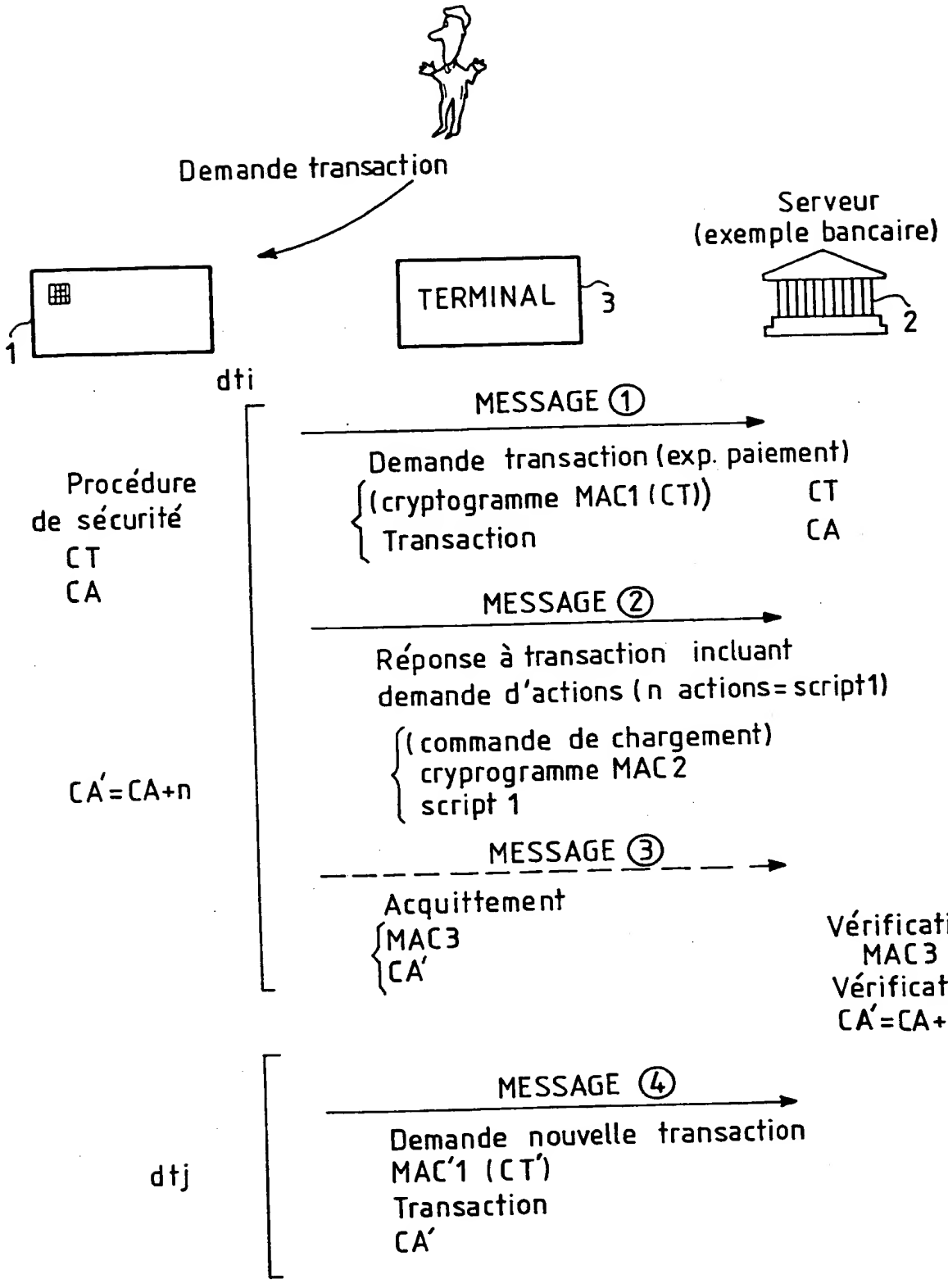
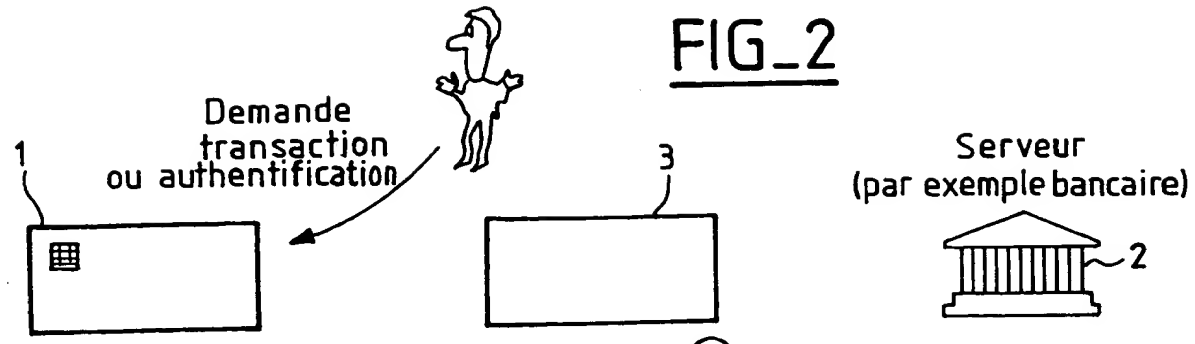

Demande transaction
Serveur
(exemple bancaire)
TERMINAL
3
1
2
dti
MESSAGE ①
Demande transaction (exp. paiement)
(cryptogramme MAC1 (CT))
Transaction
CT
CA
Procédure
de sécurité
CT
CA
MESSAGE ②
Réponse à transaction incluant
demande d'actions (n actions = script1)
(commande de chargement)
cryprogramme MAC 2
script 1
CA'=CA+n
MESSAGE ③
Acquittement
MAC3
CA'
Vérification
MAC3
Vérification
CA'=CA+n
MESSAGE ④
Demande nouvelle transaction
MAC'1 (CT')
Transaction
CA'
dtj

FIG_1

FIG_2



Application
- Calcul données d'authentification carte MAC1
- Lecture compteur d'action CA

MESSAGE ①

Demande de transaction
- MAC1
- CA
- Transaction bancaire

- Vérification MAC1
- Effectue la transaction
- Calcul donnée d'authentification serveur MAC 2
- Préparation commande de changement de paramètre script1
- Stockage CA et script1 dans DB serveur

Exemple coupure de ligne

MESSAGE ②

Réponse à transaction incluant demande d'actions (script1)

{Commande de chargement MAC2, script1

MESSAGE ③

Application
- Calcul données d'authentification carte MAC1
- Lecture compteur d'action CA

Nouvelle demande de transaction
{- MAC1, CA
{- Transaction bancaire

- Vérification MAC1
- Vérification $CA_{carte} = CA_{serveur} \Rightarrow$ annule la dernière transaction
- Calcul MAC2
- Préparation nouveau script 2
Stockage CA' et script2 dans DB serveur

MESSAGE ④

Réponse à transaction incluant demande d actions (script 2)

{Commande de chargement MAC2, Script 2

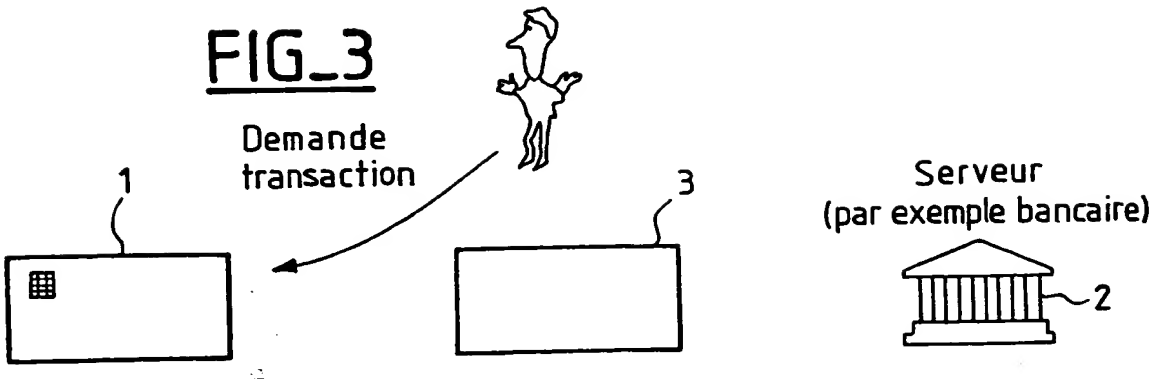
- Vérification MAC2
- Si MAC2 ok alors effectue script2
- Si script1 ok, incrémentation CA = CA +1
- Calcul MAC3 d'acquittement

MESSAGE ⑤

Acquittement MAC3, CA+1

- Vérification MAC3
- Vérification CA'=CA+1
- Effacement DB

FIG_3



Application
-Calcul données d'authentification carte MAC1
-Lecteur compteur d'action CA

MESSAGE ①

Demande de transaction
- MAC1
- CA
- Transaction bancaire

-Vérification MAC1
-Effectue la transaction
-Calcul donnée d'authentification serveur MAC 2
-Préparation commande de changement de paramètre script1
- Stockage CA et script dans DB serveur

MESSAGE ②

Réponse à transaction incluant demande d'action (script1)
{Commande de chargement
MAC2, Script1

-Vérification MAC2
- si MAC2 ok alors effectue script1
- si script1 ok incrémentation CA'=CA+1
-Calcul MAC3 d'acquittement

MESSAGE ③ (exemple coupure de ligne)

Acquittement

MESSAGE ④

Nouvelle demande d'action
-MAC1, CA'
-Transaction bancaire

Application
-Calcul données d authentification carte MAC1
-Lecture compteur d action CA'=CA+n

-Vérification MAC1
-Vérification
-CA'carte = CA+n dernière transaction OK
-Effectue la transaction courante
-Calcul MAC2
-Préparation nouveau script 2
-Stockage CA' et script 2 dans DB serveur

MESSAGE ⑤

Réponse à transaction incluant demande d'action (script 2)
{Commande de chargement
MAC2, Script2

-Vérification MAC2
- si MAC2 ok alors effectue script2
- si script 1 ok, incrémentation CA'=CA'+1
-Calcul MAC3 d'acquittement

MESSAGE ⑥

Acquittement
MAC3, CA"

-Vérification MAC3
-Vérification CA"=CA'+1
-Effacement DB